SecureCall – English

Technical Security Services

Name	NTT SecureCall Service Description – English
Owner	TSS Management
Status	APPROVED
Classification	CONFIDENTIAL-EXTERNAL
Version	V8.0
Date	01 January 2019
Review	01 June 2019

Contents

1 Introduction

1.1 Document Purpose

This Support Service Description is part of the Support Contract with the Customer. It describes the features of the SecureCall service, explains how Service Requests are processed according to priority, and sets out our escalation processes and response targets. This Support Service Description should be read in conjunction with other documents as defined below.

1.2 Support Contract Document Structure

This section describes how the contract documentation fits together.

1.3 Definitions

The following terms are used in this Support Service Description:

Term	Definition
Business Hours	Business Hours – Premium is seven days a week, 24 hours a day. Business Hours – Standard is 0900-1700, Mon-Fri
Customer	The Party purchasing the Support Service at the address set out in the Purchase Order (refer to Master Services Agreement)
ISP	Internet Service Provider
NTT Ltd.	NTT Ltd. (formerly NTT Com Security Limited) or any associate companies
Product	The software and hardware products described on the Support Certificate
Product Licence	The End User License Agreement provided by the owner of the Intellectual Property rights of a Product
Product Location	Each physical location where Product is installed, for the purposes of providing Support Service
Remote Access Troubleshooting	A particular form of troubleshooting which involves remote access and the extraction of logs and diagnostic data to aid in troubleshooting the problem reported on a Service Request
RMA	Return Material Authorization
SecureHands	A proactive remote technical assistance option to the SecureCall service
SecureCall	The NTT Ltd. Telephone Support Service
Service Request	An incident or question tracked in the NTT Ltd. ticketing system
Vendor	A manufacturer or distributor of a product or service

2 Service

2.1 Service Level

SecureCall is only delivered as a Premium service level and is delivered on a 24/7 basis.

Escalation to vendor including RMA can only happen in accordance with the underpinning Level 3 vendor support contract service level.

2.2 Scope of Support Service

The Support Service is a comprehensive service designed to address the technology lifecycle of Customer security components. It is structured as a set of baseline elements (Incident Management and Knowledge Management) and a set of optional elements available at additional cost. Further details are available in paragraphs 3.9, 3.10, 3.11 and 3.12.

Unless otherwise agreed or unless explicitly provided as part of an optional element, please note that the Support Service does NOT include:

- Provision of, or assistance with the installation of, software, hardware, upgrades, service packs, feature packs or hot fixes
- Configuration or rebuilding of systems
- Backup and restoration of systems
- Telephone based consultancy - Customer may use the SecureHands option (see paragraph 3.11)
- Telephone based training - Customer may use the SecureHands option (see paragraph 3.11)
- Support of Product versions outside of manufacturer support

  The SOC shall provide Support Service for software and hardware Product versions provided that they are still supported by their manufacturer. If a Product has reached end of support with a manufacturer, the SOC shall recommend an upgrade to a manufacturer supported version as the first step in solving a support issue. If Customer cannot upgrade, Customer may use the SecureHands option (see paragraph 3.11) to get advice from the SOC on the manufacturer unsupported technology. Product versions outside of manufacturer support will be supported under commercially reasonable efforts.
- Service Requests with a P1 or P2 prioritization where the technical issue has been raised for equipment or configuration that has NOT been successfully deployed in a production environment. Service Requests with a P3 or P4 prioritization for that equipment are within the scope of Support Service.
- Resolving incidents due to inadequate Customer product skills, technical knowledge or planning
- Misuse of the product, using product outside of manufacturer recommendations and/or not following manufacturer guidance on product limitations and supported configurations

All purchases of the Support Service by the Customer from NTT Ltd. at any time shall be covered by the Master Services Agreement and Service Description as amended from time to time. The duration of support purchased shall be as described in the relevant Support Certificate.

3 Support Service Features

3.1 Single Point of Contact

Customer is able to log Service Requests with the SOC for incidents on each product for which Support Service entitlement is current and valid.

3.2 Language Support

Commercially reasonable efforts shall be made to provide the service in English, German and French during Business Hours - Standard. Outside Business Hours - Standard Service Requests shall be placed in English and the Support Service may be delivered in English only.

3.3 Technical Support

The SOC shall provide technical incident analysis, troubleshooting and diagnosis for the supported Products.

The SOC shall initially attempt to qualify the suspected incident as an actual incident and may require the Customer to provide additional information and perform checks and tests to further isolate the suspected cause of the incident.

The Customer shall perform all tests, checks and actions requested by the SOC in order to identify a fix or work-around. Where further Customer checks are inconclusive, or are liable to affect live operation of the system, the SOC may attempt to replicate and test the suspected incident internally.

Following confirmation of an incident as actual, the SOC shall continue to investigate the fault and may require the Customer to perform further tests.

If local resolution or work-around of the incident is not achieved within reasonable timescales as agreed with the Customer, the SOC shall report the incident to the Vendor for further investigation. Part of this troubleshooting process may involve transfer of customer information and files to the Vendor.

NOTE: Escalation to vendor including RMA can only happen in accordance with the underpinning Level 3 vendor support contract service level.

During the lifecycle of a Service Request, regular communication updates shall be agreed between the SOC and Customer.

3.4 Hardware Support – including RMA

Where hardware support has been purchased by the Customer, the SOC shall provide hardware fault diagnosis and escalation to the hardware support Vendor, in accordance with the hardware support purchased.

Response times and service levels for hardware replacement vary according to the level of the hardware support purchased. (RMA shall be agreed by the Vendor and may have a daily cut off time before which the RMA must be processed). RMA response time begins once a hardware problem has been authorized by the Vendor.

NOTE: Escalation to vendor including RMA can only happen in accordance with the underpinning Level 3 vendor support contract service level.

The Customer should refer to their Support Certificate or the Technical Services SecureCall ePortal (paragraph 3.7) and/or their Account Manager to confirm details of the hardware support actually purchased.

3.5 Service Request Management

This section excludes the management of Service Requests for SecureHands and Technical Baseline Assessments which is described specifically in paragraph 3.11.

3.5.1 Service Request handling

Service Requests shall be placed with the SOC. The Service Request will be registered within the Service Request management system and the Customer will automatically receive a reference number (Service Request ID) under which the Service Request will be processed. The Customer should refer to the Service Request ID in all communications related to the specific Service Request.

3.5.2 Service Request Registration/Logging

Service Requests can be registered as follows:

Registration Method	Restrictions	Time window for registration
Telephone[1]	For all Priority issues	According to Service Level
Email[2]	For Priority 2, 3 and 4 issues only	24 x 7[3]
Portal	For Priority 2, 3 and 4 issues only	24 x 7[3]

[1] All urgent issues, for example Priority 1 Service Requests, shall be placed by telephone.

[2] Service Requests submitted by email are by default logged as a Priority 3 and shall receive an automated email acknowledgement. The default priority can be changed once the Service Request has been logged by contacting the SOC by telephone.

[3] Email and portal submitted Service Requests will be monitored on a 24/7 basis.

3.5.3 Initial Response service level

A priority shall be assigned to a Service Request when the Service Request is registered, in accordance with the table below. The table below also defines the Initial Response Targets. Initial Response means acknowledgement by a member of the SOC of the incident being logged, rather than the incident resolution.

Service Request Priority	Impact of the incident	Time window for registration
1	Production system non functional or unusable	30 minutes
2	Production system partially usable or a temporary workaround available	2 hours
3	Low impact on operation	24 hours
4	No impact on operational condition of product	2 days

3.5.3.1 Remote Access Troubleshooting

Remote Access Troubleshooting is a particular form of troubleshooting and diagnostics gathering using a remote session, based on technology such as Cisco WebEx (currently used by the SOC). If the Customer wishes to use their own remote access technology they shall inform the SOC. The use of the Customer's own technology for Remote Access Troubleshooting is at the Customer's own risk.

Remote Access Troubleshooting shall be performed only at the SOC's sole discretion. The level of access (view only/ view and control) shall be agreed with the customer.

If the Customer requires the SOC to perform other activities such as patch installation or configuration changes the Customer should use the SecureHands option (Refer to paragraph 3.11).

Customers should be aware that Remote Access Troubleshooting may have an impact on the performance of the Customer system or otherwise cause adverse effects such as device inaccessibility, device down time or network problems. The Customer confirms that NTT Ltd. shall not be liable to the Customer for any loss of services or any damages the Customer or any third party may suffer in this regard, whether direct or consequential. The Customer hereby indemnifies and holds NTT Ltd. harmless against any claim by the Customer or from a third party arising from NTT Ltd. performing diagnostics gathering.

NTT Ltd. reserves the right to make changes to the way Remote Access Troubleshooting is performed without prior notification to the Customer. Remote Access Troubleshooting sessions may be recorded by NTT Ltd. or by the Customer.

3.5.4 Service Request Monitoring

The standard Service Request monitoring process is for the SOC and Customer to agree on update intervals and expected responses.

The following table describes the process followed for Service Request monitoring:

Service Request Priority				
	1	2	3	4
Initial Service Request response	Response of 30 minutes	Response of 2 hours	Response of 24 hours	2 days
Service Request monitoring	Daily review of Service Requests by SOC			
	Automatic email alert sent to SOC on Service Requests not updated			
	SOC Team Leaders regular progress review of all open Service Requests			

3.5.5 Service Request Escalation

- The Customer should call the NTT Ltd. SOC directly and request Service Request escalation
- The SOC will then escalate the issue to the Duty Management team
- On review of the Service Request the escalation contact will action an appropriate plan dependent on the incident
- The customer contact who requested escalation will be updated on the plan and update intervals will be agreed
- If appropriate, the Customer's Account Manager (and Service Delivery Manager if applicable) will be notified at this point
- Further escalation to Director Level can be triggered if the escalation is on-going after 3 days (After 24 hours for Priority 1 (system down issues))
- All escalations are tracked centrally within the SOC
- Escalations are analysed for continual improvement of the service process

3.5.6 Service Request Closure – Root Cause Analysis

For the avoidance of doubt, troubleshooting of a Service Request does not include Root Cause Analysis reports.

Customers may request a Root Cause Analysis of an issue encountered and such requests may be processed by the SecureHands option. (Refer to paragraph 3.11)

3.6 Update and Upgrade Best Practice

The Customer is strongly advised to approach system changes and upgrades as follows in order to make best use of the Support Service and reduce down-time.

- Plan the change/upgrade in advance
  - Contact the SOC and explain what you are planning to do. The SOC may be able to advise you on the impact the change could have and on potential problems that may arise.
  - Check the Support Update Service (see paragraph 3.8) communications on the relevant topic.
- Take a backup in advance of the change/upgrade to provide a fall-back position
- Test the change/upgrade on a non-live system before implementing it on a production system
  - To address any shortfalls in resource, experience, knowledge or skillset, on-site services are available via NTT Ltd. Professional Services (see paragraph 3.9) if the Customer would like NTT Ltd. to perform changes or upgrades. Alternatively, the SecureHands option (see paragraph 3.11) can be used to provide remote assistance for change execution and/or updates and upgrades). Such services must be purchased in advance.

3.7 Technical Services SecureCall ePortal

The Technical Services SecureCall ePortal allows the Customer to:

- Open, view and update Service Requests
- Obtain details and status of Service Requests
- View reports
- View the products under support, including their maintenance/support entitlements (asset management)
- Upload and download diagnostic files required as part of the technical troubleshooting
- View documentation relating to the Support Service
- The Technical Services SecureCall ePortal is available in English language only. It can be accessed using the following link: https://support.nttsecurity.com
- Access to the Technical Services SecureCall ePortal can be requested by raising a Service Request with the SOC. The SOC can also provide the customer with the latest Portal Guide to help navigate the portal.

3.8 Support Update Service (SUS)

Support Update Service is a value-add e-mail service available to the Customer which aims to provide timely advisory information on patches, software upgrades as well as important technical bulletins for products supported under the Support Service.

NTT Ltd. is not liable for the accuracy and timely release of the information provided by Hardware and Software manufacturers. The Support Update Service is available in English only.

The Customer shall register for the SUS service. To subscribe or unsubscribe from this service, please contact the SOC.

3.9 On-Site Assistance (Cost option)

On-site Assistance is not included in the SecureCall service. If purchased, it is provided locally and shall be performed according to the local policies and delivered under the local Terms & Conditions applicable for Professional Services.

3.10 Technical Account Manager (Cost option)

By maintaining a long-term relationship with the Customer, the Technical Account Manager (TAM) gains valuable insight into the Customer security systems, organization and the overall business, information security goals and pressure points.

The TAM function is delivered during Business Hours – Standard only. A named SOC security analyst focused on the Customer account will be assigned, this security analyst will have extensive security expertise and in-depth troubleshooting skills relevant to the Customer's network profile and operating requirements.

- Technical, Single Point of Contact - the TAM shall act as a dedicated escalation contact for Support Service related issues including Service Request escalations and provide additional technical expertise and coordinate matters related to the Support Service.
- Accelerated resolution of technical issues - the TAM is notified of all Service Requests and other issues registered by the Customer, in particular the high-severity ones, where the TAM acts as an additional resource for the resolution. Working closely with the Customer, the TAM coordinates Customer incident management and problem management activities by engaging the appropriate resources to resolve issues with minimal disruption to the Customer business.
- Product Life Cycle Awareness - the TAM will ensure that supported technologies are registered for the Security Update Service (SUS) so that the Customer is aware of the Product Life Cycle and this element will be discussed at the regular meetings.
- Flexible pro-active engagement - the TAM will organize and attend Account Review Meetings at a frequency agreed with the Customer. A total of four account review meetings (one per quarter) is recommended per year. Additional or more frequent review meetings can be requested by the Customer for an additional fee. Account Review Meetings can be conducted at the Customer site (within Europe), at the SOC (currently located in the UK), allowing face to face contact with the support team, or by telephone / remote meeting. The most appropriate format of the account review meeting is to be agreed with the Customer. At the Review Meetings, the Service Request history and action plans in place will be discussed as will any future changes in Customer business or infrastructure.

3.11 'SecureHands' Remote Technical Assistance (Cost option)

The SecureHands option enables the Customer to have access to the same highly skilled team of security experts for activities beyond the baseline elements of the Support Service (as described in paragraphs 3.1 to 3.8). Therefore SecureHands can augment and supplement the Customer's own technical skills and expertise when required, and when SOC skills are available. Technologies addressed by SecureHands are a subset of the technologies covered by SecureCall. For information about eligible technologies, please contact your Account representative.

The following table illustrates some examples of SecureHands typical uses:

SecureHands Type	Typical use
Change Execution	Change implementation, Feature enablement
Remote Engineer on Request	Advice during a new install or system rebuild / Assistance beyond the scope of SecureCall / Support of equipment out of manufacturer support / Walk through of product
Tailored Request	As per Customer requirement, including Remote Access Troubleshooting (see 3.5.4.1), Root Cause Analysis (see 3.5.7)
Technical Baseline Assessment	Health check of one or more security devices
Update and Upgrade	Patch, Hotfix and minor software upgrades

SecureHands is delivered collaboratively by the SOC and the customer using a mixture of telephone assistance and remote session technology(ies) – See Remote Access Troubleshooting (3.5.3.1).

The legal Terms and Conditions pertaining to the delivery of SecureHands are those attached to the Statement of Work. A SecureHands Statement of Work (SOW) is the description of the activities (technical and other) to be performed in a SecureHands session or collection of sessions. The SOW shall be compiled by the SOC from the requirements provided by the Customer and shall be agreed by both parties and approved by the Customer before the corresponding SecureHands session(s) is(are) scheduled. When the SOW has been agreed and provided that the Customer has sufficient units to cover the activities defined in the agreed SOW, the scheduling of the SecureHands sessions will be made in agreement with the Customer. Session duration shall be agreed through the agreement of the SOW. Note that a SOW may cover multiple sessions. Unless agreed otherwise in the SOW, a SecureHands session includes any preparation or documentation time used by the SOC. A SecureHands session shall be delivered against the agreed Statement of Work and any deviations may require a re-writing of the SOW. The SOC may decline a request for SecureHands if, in the SOC's sole opinion, the technical skills are not available to meet the requirements, timescales or the scheduling requested. The Customer may be referred to the NTT Ltd. Professional Services team if the requested activity cannot be covered by SecureHands.

NTT Ltd. may contact Customers who have SecureHands units not yet covered by an agreed SOW for matters related to the scheduling of these SecureHands units.

3.11.1 SecureHands hours of service and language coverage

SecureHands hours of service (for Service Request management and for service execution) are Business Hours – Standard, unless agreed otherwise with the SOC via the SOW.

All communications with the SOC and any written documentation (including the SOW) shall be in English. Where there are available appropriate resources, SecureHands can be delivered in French or German upon customer request.

3.11.2 Procurement and SecureHands unit management

The SecureHands option shall be purchased as a cost option of the Support Service. SecureCall is a prerequisite for the purchase of SecureHands unless otherwise agreed. Units are payable in advance of the session(s) being delivered.

SecureHands units have a validity of 12 months and shall expire at the end of their validity period.

- When a SOW is agreed the units planned to be used by the SOW will be reserved against the current unit balance
- After each SecureHands session is delivered and accepted,
  - If a fixed number of units has been agreed by the parties in the SOW, the unit balance will be debited by the agreed fixed number of units for each SecureHands session.
  - In all other cases, the unit balance will be debited by the actual units used by each SecureHands session.

    SecureHands sessions are charged as the time spent for the session, in hours, rounded up to the nearest hour. If delivered within the hours of service defined in 3.11.2, one hour equates to one SecureHands unit.

    For SecureHands sessions delivered outside of Business Hours – Standard, the number of units charged per hour will differ. This will be outlined in the SOW.
- The Customer may be required to top up the unit balance if there is an insufficient number of units to cover the work defined in the SOW. NTT Ltd. shall promptly quote the Customer for the SecureHands unit difference and the Customer agrees to place a purchase order within 30 days of receipt of such a quote, to cover the SecureHands shortfall.

3.11.3 Cancellation of a SecureHands session

Where a scheduled session is cancelled by the Customer within two working days of the planned start time or where the Customer does not attend a scheduled session, the number of SecureHands units associated with the scheduled session shall be forfeited by the Customer and the SecureHands unit balance shall be immediately debited by the same number.

A scheduled SecureHands session cancelled by either party for reasons beyond its control shall be rearranged for a mutually convenient time.

3.11.4 SecureHands Service Requests management

The Customer shall place SecureHands Service Requests with the SOC by phone or by e-mail (following the same procedure as in paragraph 3.5.2). The Customer is strongly recommended to identify such a Service Request as 'SecureHands' or as 'Technical Baseline Assessment' as appropriate.

The SOC may require the Customer representative to positively identify him/herself.

The Customer is allowed to generate an unlimited number of SecureHands Service Requests; this is subject to 'fair use' in NTT Ltd. sole opinion.

3.11.5 SecureHands Service Level Targets

The following Service Level targets shall apply:

Description	Response Time Targets
Initial Response to a SecureHands Service Request	Change implementation, Feature enablement
SOW Response target	2 working days after request
Scheduling of a SecureHands session (provided an agreed SOW is already in place)	3 working days after SecureHands session request

3.11.6 Completion and Acceptance of SecureHands sessions

After a SecureHands session has been completed, the SOC shall send a SecureHands session completion statement to the customer that:

- Details the time and the associated number of SecureHands units consumed by the SecureHands session
- Provides the Customer with the current SecureHands unit balance
- Seeks feedback from the Customer on the SecureHands session

The acceptance of a SecureHands session shall be done in accordance with the Acceptance Criteria defined in the SOW. Unless agreed otherwise in the SOW or unless the Customer raises a query regarding the SecureHands session, a SecureHands sessions shall be considered accepted by the Customer 2 working days after the 'SecureHands session completion statement' has been sent.

3.11.7 SecureHands service credits

Should the Customer raise a query related to the acceptance of a SecureHands session, within 2 working days after the 'SecureHands session completion statement' has been sent, the SOC management will investigate the query collaboratively with the Customer. Within 5 working days of the query being received from the Customer, NTT Ltd. may, at its sole discretion, cancel the debit from the Customer's SecureHands unit balance of all or part of the number of SecureHands units used by the SecureHands session queried.

3.12 Technical Baseline Assessments (Cost option)

3.12.1 Service Option Overview

Technical Baseline Assessments provide a health-check of a customer's critical security devices, using industry best practice to assess that these systems are fit for use.

Technical Baseline Assessments are delivered using the 'SecureHands' Remote Technical Assistance delivery mechanism (see paragraph 3.11), which includes an agreed Statement of Work (SOW), against identified assets. The legal Terms and Conditions pertaining to the delivery of the Technical Baseline Assessments are those attached to the Statement of Work. As defined and agreed in the SOW, a report may be provided for each assessment with the findings and recommendations for improvement if any.

The description of the Technical Baseline Assessment below is provided as general scope and guidelines. In the case of discrepancy between the description below and the SOW, the SOW shall have precedence.

A security device Technical Baseline Assessment is aimed at identifying inadequacies and vulnerabilities in a security device before these become critical. The SOC will identify, classify and prioritize issues according to criticality, impact and overall severity and recommend remedial actions going forward. These remedial actions will include any recommended changes and an impact analysis for each recommendation. All of this information will be presented in a written report to the customer. Further work can then be arranged through SecureHands or Onsite Assistance.

Assessments are unique to each product and may include review of hardware, software, networking, high availability, system services and administration.

3.13 Security Assessment Scan (SAS) (Cost Option)

3.13.1 Security Assessment Scan

The Security Assessment Scan provides the Customer with a report on vulnerabilities that a potential hacker could find and exploit.

The assessment consists of an external unauthenticated scan of a customer's perimeter IP addresses as defined by the Customer and agreed in the Statement of Work. A maximum of 25 externally accessible IPs will be scanned (more IPs can be scanned upon request subject to agreement with the SOC). A maximum of two scans of the same group of IPs are included in one engagement:

1. Scan 1. This is the initial scan performed on IP addresses provided by a customer and will form the basis of the report and any following recommendations.
2. Scan 2. This scan is a remediation scan that should be completed after all required remediation has been completed by the customer or with help of SecureHands units (see 3.11) this is to ensure detected vulnerabilities from the first scan have been addressed, the second scan will not include any additional assets or new vulnerabilities. The second scan must be requested within 30 days of the report review and must be performed within 45 days of the report review. This is the Customer's responsibility to request.

Following the scan,

- A report is provided to the nominated Customer contact(s) (Customer's IPS may affect scan capability and report outcome).
- A SOC Security Analyst will review the report with the nominated Customer contact(s) providing additional advice on protecting against vulnerabilities. The review will be scheduled within Business Hours - Standard. Both the vulnerability report and review will be delivered in English language.

Scans can be scheduled to fit with customers' requirements subject to available SOC skills. If rescheduling of the engagement is needed the SOC should to be notified two business days before the scheduled scan.

Vulnerability assessments can be purchased at any time and credits are valid for 12 months from NTT Ltd. receipt of operational company order.

3.13.2 Security Assessment Scan Request Management

The Customer shall place Vulnerability Scan Service Requests with the SOC by phone or by e-mail (following the same procedure as in paragraph 3.5.2). The Customer is strongly recommended to identify such a Service Request as 'Vulnerability Assessment'.

3.13.3 Security Assessment Scan Level Targets

The following Service Level targets shall apply:

Description	Response Time Targets
Initial Response to a Security Assessment Scan Request	8 Working hours
Scheduling of Scan	3 working days following receipt of signed SOW populated with customer IP addresses and contact details

4 Security Technology Training (STT)

4.1 Training Outline

STT will deliver remote training via WebEx for a maximum of 5 people (larger group training can be requested from STT).

The sessions will be delivered by one of our highly certified and experienced engineers and are designed to be no longer than 3 hours. The session will include presentation deck, real hands on lab examples and the possibility to ask questions.

For further details please refer to Security Technology Training (STT) Catalogue document.

All the material used in the training sessions are created by NTT Ltd. and does not represent the official certification training form the related vendors.

5 Responsibilities

5.1 Customer Responsibilities

5.1.1 General Customer Responsibilities

Customer shall ensure that NTT Ltd.'s actions undertaken in connection with the Support Service shall be deemed to be authorized by the Customer and all third parties for the purposes of any applicable legislation in any jurisdiction in which the Customer operates and any contract governing the use of such network and systems.

The Customer warrants that NTT Ltd. shall be entitled to act upon all information and directions supplied to NTT Ltd. by any of the Customer's employees.

Applicable to all features and options of the Support Service, the Customer shall:

- Have valid Product Licences for all Products supported and ensure that these are at all times in compliance with all Product Licence terms and conditions
- The customer must have appropriate admin access to any admin/management gui/console for trouble shooting and management of the solution or device covered under SecureCall support
- Ensure that renewal of any support service agreement takes place in a timely fashion
- Be responsible for timely installation of patches and updates where reasonable
- Take appropriate regular backups of all data on the supported devices
- Co-operate with SOC requests for positive identification of Customer representatives
- Maintain personnel with adequate technical expertise and training to assist NTT Ltd. in providing troubleshooting and problem resolution. The customer shall restrict access to the SOC to such adequately skilled personnel and shall notify the SOC of new starters/movers/leavers for access management purposes
- Provide sufficient information to enable the SOC to uniquely identify the product under support and the appropriate support contract such as licence key, mac address or serial number
- Co-operate with NTT Ltd. in the troubleshooting and diagnosis of an incident
- Provide NTT Ltd. or NTT Ltd. designated subcontractors with such access and written permissions to the Customer's infrastructure and applications as may be reasonably necessary for the performance of the Support Service and ensure that such access is in accordance with the Customer Information Security policies
- Be available to be contacted by the SOC or Vendor and to attend to the activities necessary for the progression of a Service Request as requested by NTT Ltd. or the Vendor, and provide timely and accurate technical information to NTT as requested by NTT or the Vendor
- In the case of Remote Access Troubleshooting or SecureHands, be present for the entire duration of the session and have physical access to the device at all times during the SecureHands session

In the event that the Customer fails to comply with any of the obligations set out above, NTT Ltd. and its sub-contractors shall have no liability arising from any failed attempt to provide the Support Service and NTT Ltd. shall be entitled to such costs as are charged by a sub-contractor to NTT Ltd. to provide or rectify the Support Service, which amount is agreed as representing reasonable wasted costs incurred by NTT Ltd.

The customer also has the following additional responsibilities specific to the support of hardware devices:

- To ensure NTT Ltd. are advised of any change in the Product Location(s) by giving written notice to NTT Ltd. as soon as it occurs and no later than 30 days prior to any site visit
- To return to the Vendor (as instructed in the RMA process) the faulty hardware as soon as reasonably practical. In case the Customer fails to return the faulty hardware within the time specified in their hardware contract, NTT reserves the right to charge the Customer a fee equivalent to the fee incurred by NTT Ltd. from the Vendor for this failure to return hardware
- To pay transport and custom costs for the RMA process described above (when these are not covered by the hardware support Vendor)

5.1.2 Remote Access Troubleshooting and SecureHands

The customer shall:

- For SecureHands, co-operate with the SOC in the production of an accurate Statement of Work (SOW) and provide answers to all SOC questions pertaining to the production of the SOW
- Have a contingency or roll back plan, that shall be communicated to the SOC as part of the SOW, in case a remote session is lost and cannot be re-established during a SecureHands session or in case the activities of a SecureHands session are not successful or do not yield the expected outcome
- Make sure that the system(s) are backed up adequately and are able to be restored to the 'last known good' state if required. The restoration of the system is the Customer's responsibility
- Provide a single technical point to coordinate access to relevant equipment and personnel
- immediately after a SecureHands session, reset any credentials communicated or used during the SecureHands session

Other prerequisites and Customer responsibilities may be agreed in the SOW. In case of conflict between this document and the SOW, the SOW shall apply.

5.2 NTT Ltd. Responsibilities

5.2.1 General NTT Ltd. Responsibilities

- NTT Ltd. is not liable to make any changes to third party or Customer developed hardware or software that may be necessary as a result of any software patches or software updates recommended by NTT Ltd. or the original manufacturer of the product
- NTT Ltd. is not liable to make any changes to third party or Customer developed hardware or software that may be necessary in order to take advantage of additional or enhanced facilities and capabilities provided with new releases of the supported product

NTT Ltd. shall:

- Use reasonable commercial effort to document, in their Service Request Management System, the actions performed by the SOC
- Use reasonable care whilst performing troubleshooting and diagnostics
- End any Remote Access Troubleshooting session in agreement with the Customer, unless the session was initiated by the Customer

To ensure a consistent level of service quality, the SOC will:

- Monitor the agreed service levels
- Conduct regular internal service reviews for Continual Service Improvement
- Seek Customer feed-back and input via Customer Satisfaction Survey

For Technical Baseline Assessments the SOC shall:

- Ensure all devices are returned to pre-assessment status following the Technical Baseline Assessment
- Present the Technical Baseline Assessment findings to the Customer following the assessment, in the format agreed in the SOW

Together we do great things